Apple iPhone 15+ – Firmware/Baseband Compromise Submission for CISA

Submitter: John R. Fouts

Date: May 25, 2025

Location of Purchase: T-Mobile, Hurstbourne Parkway, Louisville, KY

T-Mobile Associate: Giselle

Case Reference: CCASE0092315 (T-Mobile Infrastructure)

Device and OS Details

Device: Apple iPhone 15+
Purchased: Summer 2024 (new, last inventory unit per staff)
Operating Systems Affected: iOS 17 and iOS 18
Condition: Factory-sealed, no third-party tampering

Indicators of Compromise

1. Unauthorized Microphone Activation

- Microphone activated repeatedly with no user input
- iOS Privacy logs showed 'Microphone recently used by: Unknown'
- No apps granted microphone access; all Apple voice features (Siri, Dictation, Voice Control) disabled
- Activation occurred offline, including in Airplane Mode
- Suggests baseband- or firmware-level access bypassing app-layer controls

2. Call Interception

- Call to White House switchboard was intercepted or rerouted
- No confirmation of successful routing or expected connection

- No SIM card involved; device uses internal eSIM/baseband
- Suggests man-in-the-middle attack, rogue tower, or baseband compromise

Context and Request for Action

This submission is connected to previously reported incidents under T-Mobile and ASUS hardware compromise (see case CCASE0092315 and related firmware submission). Device behavior, including DNS redirection, Airplane Mode surveillance, and cross-vendor compromise patterns, suggests coordinated infrastructure-level threat.

I respectfully request CISA escalate this matter to the appropriate firmware and supply-chain review divisions. This device behavior represents a threat to critical communications and affects a federally protected individual under ADA, VAWA, and 1915(c).